様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　４ 年　 ６ 月 ２７ 日現在

機関番号：２１６０２
研究種目：基盤研究(C)（一般）
研究期間：2019～2021
課題番号：１９Ｋ１１９６７

研究課題名（和文）セマンティックなセキュリティ情報モデリングとセキュリティ管理自動化への応用

研究課題名（英文）Semantic Security Information Modeling and Security Management Automation

研究代表者
中村　章人（Nakamura, Akihito）

会津大学・コンピュータ理工学部・上級准教授

研究者番号：７０３５７６６４

交付決定額（研究期間全体）：（直接経費）　　2,000,000円

研究成果の概要（和文）：セキュリティ脆弱性とそれを狙うサイバー攻撃の情報モデリングに取り組み、機械可読可能な情報記述方式を定義した。この情報に基づいて、脆弱性が発現する環境を仮想空間内に自動構築し、攻撃も自動で実行するソフトウェアを開発した。また、ネットワークシステムのセキュリティテストを自動化する方式を確立し、ネットワークパケットを操作することでさまざまな障害やサイバー攻撃を疑似的に発生させることができるネットワークエミュレータを開発した。

研究成果の学術的意義や社会的意義
セキュリティ情報の機械可読性および意味レベルの相互運用性を高めて、これを利用したセキュリティ対策の自動化や効率化を促進する。また、セキュリティ対策プロセスの自動化方式およびツールは、ソフトウェア開発者やシステム管理者のセキュリティテストの効率化に資すると共に、セキュリティ診断の自動化や、セキュリティ教育・学習用の環境構築などに有効なツールとなり得る。

研究成果の概要（英文）：Worked on information modeling of security vulnerabilities and cyber attacks targeting them, and defined a machine-readable information description scheme. Based on this information, we developed software that automatically constructs an environment in a virtual space where the vulnerability is reproduced and automatically executes the attack. Furthermore, we established a method to automate security testing of network systems and developed a network emulator that can emulate various failures and cyber attacks by manipulating network packets.

研究分野：情報セキュリティ

キーワード：サイバーセキュリティ　脆弱性　ネットワークエミュレーション　セキュリティテスト　システム管理

様　式　C－１９、F－１９－１、Z－１９（共通）

１．研究開始当初の背景

(1) 情報技術やインターネットの発展と普及に伴い、サイバーセキュリティが重要な社会問題と捉えられるようになってきた。セキュリティ対策の必要性が高まる一方で、対策のプロセスは人手に頼る部分が多く、セキュリティ対策の正確性や即応性に問題がある。

(2) セキュリティ対策に必要な情報（いわゆる脆弱性情報など）は人間向けに自然言語で記述されており、セキュリティツールを用いた対策プロセスの自動化・効率化に利用できない。

２．研究の目的

(1)グローバルに共有可能な精緻で相互運用性の高い機械可読なセキュリティ情報の記述方法を確立する。このような形式の情報を普及・流通させることで、ベンダ・ツールへの依存を減らし、データ中心のセキュリティ自動化を促す。

(2) 上記の機械可読なセキュリティ関連情報を利用して、セキュリティ対策プロセスの自動化を図る。特にセキュリティテストや脆弱性診断の自動化手法を研究し、ソフトウェア開発者やシステム管理者のセキュリティ対策を支援する自動化ツールを開発する。

３．研究の方法

(1) セキュリティ対策に利用する情報の機械可読性および意味レベルでの相互運用性を高めて、様々なセキュリティアプリケーションやサービスから共通的かつ汎用的に利用できるセマンティックなセキュリティ情報モデルを構築する。

(2) 上記の機械可読なセキュリティ関連情報を利用して、セキュリティ対策のプロセスを自動化するツールを開発する。特にセキュリティテストや脆弱性診断に着目し、必要となる環境や機能・プロセスを分析し、モデリングを行って自動化の手法を研究する。最終的に、ソフトウェア開発者やシステム管理者のセキュリティ対策を支援する自動化ツールを開発する。

４．研究成果

(1) 脆弱性とそれに対応するサイバー攻撃の情報モデリングに取り組み、機械可読可能なデータ構造を定義した[1]。データ記述には汎用性の高い YAML 言語を用いた。まず、攻撃者、エクスプロイト（攻撃コード）、攻撃対象ホスト、ネットワークなどの主要な要素から成るサイバー攻撃の全体像をモデル化した。次に、攻撃対象ホスト（被攻撃ホスト）の構成要素および攻撃コードを分析して、これらを記述する YAML のデータ構造を定義した。被攻撃ホストの構成は、OS 単体で発現する脆弱性だけでなく、特定のアプリケーションソフトウェアやその特定の構成下で発現するもの、さらにデータベースや Web ページなどのコンテンツを必要とするものまでいくつかのクラスを定義し、柔軟な記述ができるようにした。最終的に、脆弱性（Vulnerability）、被攻撃ホスト（Host）、攻撃方法（Attack）の三つの主要素とそれぞれの詳細から成る脆弱性のテストメタデータユニット（Testing Metadata Unit: TMU）として構造化した（**図** 1）。このデータを利用するツールの要求が必ずしもすべての要素を必要としない場合が考えられるため、被攻撃ホストと攻撃方法は省略可能としている。よって、それぞれを省略した場合を含めて 3 種類の構成を提供する。図 2 と図 3 に、Wordpress サーバの脆弱性を発現するための被攻撃ホストの構成と Metasploit を用いた攻撃方法の記述の例を示す。

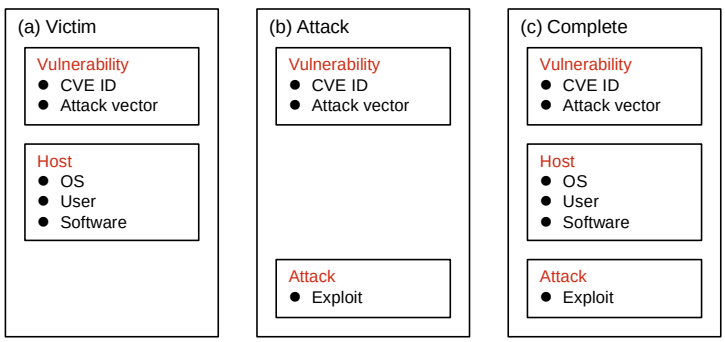

図 1: 脆弱性のテストメタデータユニット（Testing Metadata Unit: TMU）; (a) 被攻撃ホストモデル, (b) 攻撃方法モデル, (c) 完全モデル

```yaml
vulnerability:
  cve: CVE-2017-5487
  attack_vector: remote

host:
  os:
    name: ubuntu
    version: 18.04.1
  user:
    - name: mysql
      password : "mysql"
      shell: /bin/bash

  software :
    - name : gcc
    - name : wordpress
      vulnerability: true
      version: 4.7.1
      method: source
      config:
        post_config :
          - name : setting_db
            mysql_database :
              database : wordpress
              login_user : root
              login_password : "***"
              config_file : /etc/mysql/my.cnf
          - name : setting_user
            mysql_user :
              user : wordpressuser
              password : "***"
              host : localhost
              config_file : /etc/mysql/my.cnf
      software:
        - name : httpd
          version : 2.4.43
        - name : mysql-server
```

図 2: 脆弱性のテストメタデータユニットの例 1（Wordpress の脆弱性と被攻撃ホストの構成）

```yaml
vulnerability:
  cve: CVE-2017-5487
  attack_vector: remote

attack:
  exploit_method : http
    request:
      url: http://192.168.177.177/wordpress
         /index.php /wp-json/wp/v2
          /posts/1/?id=1AAA
      method: post
      header:
        Accept : application/json
        Content-type: application/json
      body:
        title : "Hello World CVE-2017-5487"
        content: "Vulnerability in Wordpress
                  version 4.1"
```

図 3: 脆弱性のテストメタデータユニットの例 2（Wordpress への攻撃方法）

(2) (1)で示した脆弱性 TMU を読み込んで解釈し、仮想空間内にサイバー攻撃実行環境を構築するソフトウェアを開発した[1]。まず、被攻撃ホストの記述に基づき仮想計算機を作成し、指定の OS および必要なソフトウェアのインストールと設定を行う。次に、攻撃方法の記述に基づいて攻撃コードをインストールする。最後に攻撃を実行して、攻撃の成否や被攻撃ホストの構成などについてのレポートを出力する。すなわち、与えられた脆弱性 TMU に対して、仮想空間内で環境構築から攻撃の実施およびレポート出力までの一連のプロセスをすべてソフトウェアで自動化した。ユーザは脆弱性の識別子（CVE ID）を指定するだけで、あとはツールがすべて自動実行する。いくつかの脆弱性について実際に TMU を記述してソフトウェアの動作確認を行い、実用に資することを確認した。オープンソースソフトウェアとして GitHub 上で公開している。これらの成果は、ソフトウェア開発者やシステム管理者のセキュリティテストの効率化に資すると共に、セキュリティ診断や構成管理の自動化、セキュリティ教育・学習用の環境構築などに有効なツールとなり得る。

(3) ネットワーク接続されたシステムのセキュリティテストを自動化する方式を研究し、それを実現するソフトウェア（ネットワークエミュレータと呼ぶ）を開発した[2]。本ネットワークエミュレータは、ネットワーク中を流れるパケットを中継時に操作することで、さまざまな障害やサイバー攻撃を疑似的に発生させることができる（図 4）。例えば、パケットを遅延させることでサーバの負荷上昇やネットワーク輻輳を、パケットを廃棄することでサーバやクライアントの停止を、パケットの内容を書き換えることで中間者攻撃を、送信されていないパケットを挿入することでサービス妨害攻撃を模擬する。このようなパケット操作を、システムテストで想定するシナリオに基づいて高精度に再現できるようにした。テストシナリオは、機械可読な形式であらかじめ記述しておき、システムに入力できる。記述言語には多くのプログラミング言語で利用できる JSON を用いた。これによって、さまざまなテストシナリオを何度でも正

確に自動で再現できるようになり、ソフトウェア開発者やシステムインテグレータが行うテストの効率と精度が高まる。本方式は、TCP/UDP/IP のプロトコルに対応しているため、インターネットで通信可能なあらゆる種類のコンピュータシステムのテストに利用できる。特に、組込機器や IoT（Internet of Things）と呼ばれる内部構成を自由に変更できないシステムのテストに有効である。性能評価を行い、非常に高い精度で障害やサイバー攻撃を再現できることを確認した。

＜引用文献＞

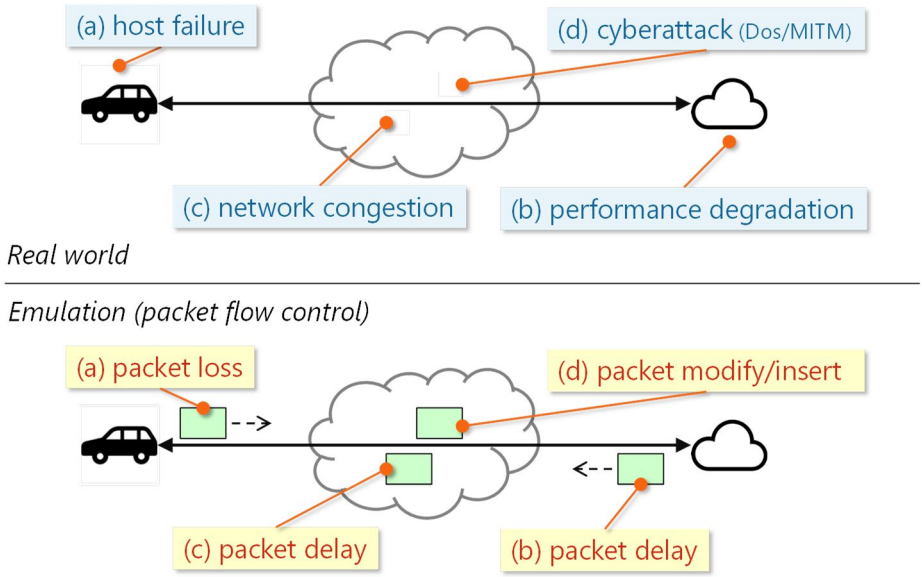

図 4: ネットワーエミュレータのパケット制御による障害・サイバー攻撃の再現

[1] Kohei Akasaka, Akihito Nakamura, "Reproducible Software Vulnerability Testing with IaC", 7th International Conference on Computational Science and Computational Intelligence (CSCI'20), IEEE CPS, NV, USA, Dec 2020.
[2] Keita Yoshida, Akihito Nakamura, "Network Emulator Approach to Testing Internet of Everything", World Congress in Computer Science, Computer Engineering, and Applied Computing (CSCE'21), NV, USA, July, 2021.

５．主な発表論文等

〔雑誌論文〕　計0件

〔学会発表〕　計2件（うち招待講演　0件／うち国際学会　2件）

１．発表者名 Keita Yoshida, Akihito Nakamura
２．発表標題 Network Emulator Approach to Testing Internet of Everything
３．学会等名 World Congress in Computer Science, Computer Engineering, and Applied Computing (CSCE'21)（国際学会）
４．発表年 2021年

１．発表者名 Kohei Akasaka, Akihito Nakamura
２．発表標題 Reproducible Software Vulnerability Testing with IaC
３．学会等名 7th International Conference on Computational Science and Computational Intelligence (CSCI ' 20)（国際学会）
４．発表年 2020年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

Automation tool for software vulnerability testing https://github.com/uoanlab/vultest Network Emulator for Testing Internet of Everything https://github.com/uoanlab/netemu-poc

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関